Ref. 1

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11032088 A**

(43) Date of publication of application: **02 . 02 . 99**

(51) Int. Cl **H04L 12/66**
G06F 13/00
G06F 13/00
H04L 12/46
H04L 12/28
H04L 12/24
H04L 12/26

(21) Application number: **09186850**

(22) Date of filing: **11 . 07 . 97**

(71) Applicant: **HITACHI LTD**

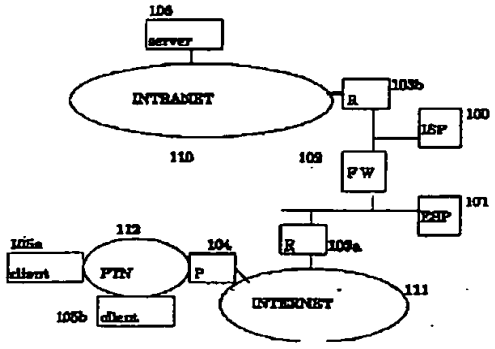
(72) Inventor: **KONDO TAKESHI**
NAKADA YUKIO
AKAOSUGI TAKASHI

(54) **NETWORK SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To execute safe communication via a fire wall(FW) without altering an application program by performing communication with a second data communication means and transferring the data of a specified application program without mutually constructing a data transfer path and changing a specified program on a computer.

SOLUTION: An FW 102 is provided with a socket-processing part and a TCP/IP processing part, and a main processing part is a circuit gateway type operated as the application program(AP) of the FW 102, transmits and receives the ID of a connection destination and a transmitter and relays the data from the transmitter confirmed by an authentication processing part. An ESP 101 is composed of an ISP protocol processing part for performing the communication with an ISP 100 and a client protocol processing part for performing the communication with a client, and in the case of coping with the various APs, only setting information needs to be changed by using a text editor, so that development cost is reduced and extendability is high.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－32088

(43)公開日　平成11年(1999)２月２日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/66		Ｈ０４Ｌ	11/20	Ｂ
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ｚ
		３５７			３５７Ｚ
Ｈ０４Ｌ	12/46		Ｈ０４Ｌ	11/00	３１０Ｃ
	12/28			11/08	

審査請求　未請求　請求項の数18　ＯＬ　（全 21 頁）　最終頁に続く

(21)出願番号　特願平9－186850

(22)出願日　平成９年(1997)７月11日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　近藤　毅
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所システム開発研究所内

(72)発明者　中田　幸男
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所システム開発研究所内

(72)発明者　赤尾杉　隆
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　武　顕次郎

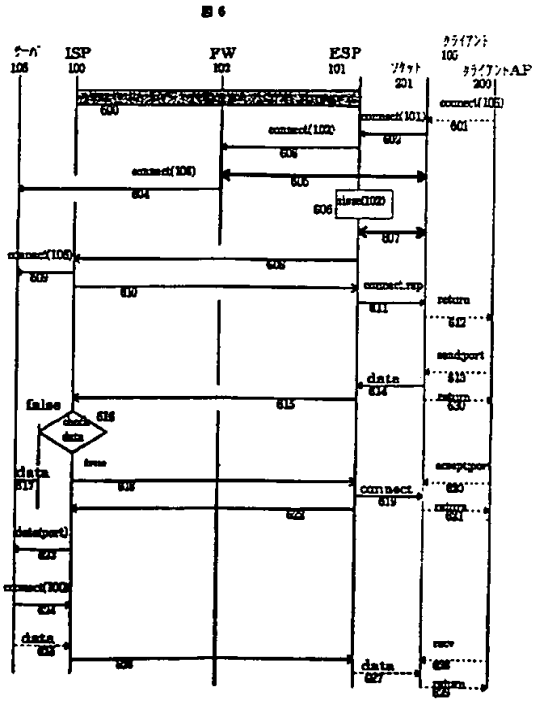
(54)【発明の名称】　ネットワークシステム

(57)【要約】

【課題】　動的にアサインされる通信ポートを使用するＡＰを、ＦＷで仕切られたネットワーク間で、そのＡＰを変更することなく動作させる。

【解決手段】　ＦＷ１０２で保護されたイントラネット１１０に接続するＩＳＰ１００とＦＷ１０２で保護されていないインターネット１１１に接続するＥＳＰ１０１を設ける。ＥＳＰ－ＩＳＰ間で通信路を確立し、ＩＳＰからＥＳＰへアクセス情報を配布、初期化終了後、ＡＰのデータをＥＳＰ－ＩＳＰ間の通信路で中継する。

【効果】　ＦＷシステムの開発コストが低減でき、かつ、ＡＰ毎のきめ細かいアクセス制御を行うことができる。



【特許請求の範囲】

【請求項１】　相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構成され、前記サーバ計算機と前記クライアント計算機上のアプリケーションプログラムとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記汎用アクセスチェック装置により保護されたネットワークと接続される第１のデータ通信手段と、前記汎用アクセスチェック装置で保護されていないネットワークに接続される第２のデータ通信手段と、前記第１と第２のデータ通信手段の相互間にデータ転送パスを構築する手段と、前記クライアント計算機上の特定アプリケーションプログラムを変更することなく前記第２のデータ通信手段と通信を行って前記特定アプリケーションプログラムのデータを転送する手段と、前記第１の通信手段と第２の通信手段との間のデータ転送パスを用いて前記特定アプリケーションプログラムのデータを中継するデータ中継手段と、特定アプリケーションプログラムのデータ内容に基づいて前記特定アプリケーションプログラムのデータ中継手段を制御する手段とを備えたことを特徴とするネットワークシステム。

【請求項２】　クライアント計算機と汎用アクセスチェック装置との間の通信路が暗号化されており、前記第１のデータ通信手段が特定アプリケーションプログラムのデータ内容の判定機能を持つことを特徴とする請求項１記載のネットワークシステム。

【請求項３】　前記第１のデータ通信手段と第２のデータ通信手段とが独立した専用装置として構成されることを特徴とする請求項１または２記載のネットワークシステム。

【請求項４】　前記第１のデータ通信手段と第２のデータ通信手段との間のデータ転送パスを用いて前記データ中継手段を制御する手段への初期化情報を配布する機能を備えたことを特徴とする請求項１、２または３記載のネットワークシステム。

【請求項５】　クライアント計算機と汎用アクセスチェック装置との間で認証データを中継する認証データ中継装置を備え、前記汎用アクセスチェック装置に認証機能を備え、認証が終えたらその認証結果に基づいて前記第１のデータ通信手段と第２のデータ通信手段との間のデータ転送パスを用いてクライアント計算機のデータの中継を実行することを特徴とする請求項１ないし４のうちいずれか１記載のネットシステム。

【請求項６】　前記第１のデータ通信手段と第２のデータ通信手段との間のデータ転送パスを暗号化する機能を備えたことを特徴とする請求項１ないし５のうちいずれか１記載のネットワークシステム。

【請求項７】　前記第１のデータ通信手段または第２のデータ通信手段とクライアント計算機との間のデータを暗号化する機能を備えたことを特徴とする請求項１ないし６のうちいずれか１記載のネットワークシステム。

【請求項８】　前記第１のデータ通信手段と第２のデータ通信手段との間のデータ転送パスを用いて、第１のデータ通信手段と第２のデータ通信手段との間でアプリケーションプログラムデータの転送制御用の情報を送受信することを特徴とする請求項１ないし７のうちいずれか１記載のネットワークシステム。

【請求項９】　前記第１のデータ通信手段と第２のデータ通信手段との間の１つのデータ転送パスを用いて、複数の特定アプリケーションプログラムデータを中継することを特徴とする請求項１ないし８のうちいずれか１記載のネットワークシステム。

【請求項１０】　前記第１のデータ通信手段と第２のデータ通信手段との相互間で、相互を認証する機能を備えたことを特徴とする請求項１ないし９のうちいずれか１記載のネットワークシステム。

【請求項１１】　前記第１のデータ通信手段と第２のデータ通信手段との間を直接伝送路で接続し、前記第１のデータ通信手段と第２のデータ通信手段との間のデータ転送パスを、前記伝送路を用いて構築したことを特徴とする請求項１ないし１０のうちいずれか１記載のネットワークシステム。

【請求項１２】　前記クライアント計算機は、汎用アクセスチェック装置を介してサーバ計算機と接続するか、第２のデータ通信手段を介して接続するかを振り分ける機能を有することを特徴とする請求項１ないし１１のうちいずれか１記載のネットワークシステム。

【請求項１３】　前記第１のデータ通信手段と第２のデータ通信手段との間のデータ転送パスを、第２のデータ通信手段が複数の第１のデータ通信手段との間に確立させることを特徴とする請求項１ないし１２のうちいずれか１記載のネットワークシステム。

【請求項１４】　前記第１のデータ通信手段と第２のデータ通信手段との間のデータ転送パスを、第１のデータ通信手段が複数の第２のデータ通信手段との間に確立させることを特徴とする請求項１ないし１２のうちいずれか１記載のネットワークシステム。

【請求項１５】　前記汎用アクセスチェック装置により保護されているネットワークにおけるセキュリティポリシー情報を、前記第２のデータ通信手段に前記第１のデータ通信手段と第２のデータ通信手段との間のデータ転送パスを用いて反映させる機能を備えたことを特徴とする請求項１ないし１４のうちいずれか１記載のネットワークシステム。

【請求項１６】　相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構

成され、前記サーバ計算機と前記クライアント計算機上のアプリケーションプログラムとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記汎用アクセスチェック装置により保護されたネットワークと前記汎用アクセスチェック装置で保護されていないネットワークとの両方に接続される特定アプリケーションプログラム用アクセスチェック装置と、前記クライアント計算機上の特定アプリケーションプログラムを変更することなく前記特定アプリケーションプログラム用アクセスチェック装置と通信を行い、前記特定アプリケーションプログラムのデータをクライアント用アプリケーションプログラムを変更することなく前記アプリケーションプログラム用アクセスチェック装置に転送する手段と、前記特定アプリケーションプログラム用アクセスチェック装置で特定アプリケーションプログラムのデータを中継する中継手段と、特定アプリケーションプログラムのデータ内容に基づいて前記特定アプリケーションプログラムの中継手段を制御する手段とを備えたことを特徴とするネットワークシステム。

【請求項１７】　相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構成され、前記サーバ計算機と前記クライアント計算機上のアプリケーションプログラムとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記アクセスチェック装置は、ネットワークと直接接続されない汎用的なアクセスチェックプログラムと、保護されたネットワークを用いて通信を行う第１のプログラムと、保護されていないネットワークを用いて通信を行う第２のプログラムと、前記３つのプログラム相互間の通信手段と、特定アプリケーションプログラムのデータ内容に応じて汎用的なアクセスチェックプログラムを介したデータ中継処理を制御する手段と、前記クライアント計算機上の特定アプリケーションプログラムを変更することなく前記アクセスチェック装置との通信を行う手段とを備えたことを特徴とするネットワークシステム。

【請求項１８】　相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構成され、前記サーバ計算機と前記クライアント計算機上のアプリケーションプログラムとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記汎用アクセスチェック装置により保護されているネットワークに接続される第１の装置と前記と異なる汎用アクセスチェック装置で保護されたネットワークに接続する第２の装置とを設け、前記複数の汎用アクセスチェック装置を介して前記第１と第２の装置との間にデータ転送パスを構築する手段と、前記クライアント計算機上の特定アプリケーションプログラムを変更することなく、前記第２の装置と通信を行い、前記特定アプリケーションプログラムのデータを前記第２の装置に転送する手段と、第１の装置と第２の装置との間のデータ転送パスを用いて特定アプリケーションプログラムのデータを配送する手段と、特定アプリケーションプログラムのデータ内容に基づいて前記特定アプリケーションプログラムのデータ転送手段を起動する手段とを備えたことを特徴とするネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークシステムに係り、特に、イントラネットやインターネット等のネットワークを利用し、すでに使用している多様なアプリケーションプログラム（以下、ＡＰという）を改造することなく使用して、安全な通信を行うことのできるセキュリティ性の高いネットワークシステムに関する。

【０００２】

【従来の技術】ネットワークへの不正なアクセスを防止することによりネットワークシステムの安全性の向上を図ることのできる従来技術として、ＦＷ(Fire Wall)構築技術が知られている。このＦＷ構築技術には、アプリケーションゲートウェイ（以下、ＡＰＧＷという）、サーキットゲートウェイ（以下、ＳＣＧＷという）、パケットフィルタ等が知られてる。

【０００３】パケットフィルタに関する従来技術として、例えば、特開平５－３２７７１７号公報に記載された技術が知られている。この従来技術は、端末アドレスとポート番号との組でパケットをフィルタするというものである。また、ＳＣＧＷに関する従来技術として、Ｉnternet－Draftsにおける“ＳＯＣＫ Protocol Version 5”に記載された技術が知られている。

【０００４】その他、前述したようなネットワークへの不正なアクセスの防止だけでなく、ネットワーク上のデータの盗聴や改竄を防止するため、通信路を暗号化するＶＰＮを構築可能とするＦＷも知られており、この実現の技術としてトンネル技術によるＶＰＮを構築することも知られている。

【０００５】

【発明が解決しようとする課題】前述したＳＣＧＷ方式のＦＷは、通信ポートが固定でないＡＰを、既存のＡＰを改造することなく実現することができないという問題点を有し、また、ＡＰＧＷと併用したパケットフィルタＦＷは、通信ポートが固定でないＡＰをサポートすることができるが、そのためには、ＡＰ毎に対応したＡＰＧＷを用いなければならず、その開発コストが高く、また、性能的に劣っているという問題点を有している。

【０００６】本発明の目的は、前述した従来技術の問題点を解決し、ＳＣＧＷ方式のＦＷを用いたネットワークシステムにおいて、通信ポートが固定でないＡＰを、既

存のＡＰを無改造なまま使用してＦＷが備えるアクセスチェック機能を実現することを可能とし、開発コストが低く性能的に劣らないセキュリティ性能を持ったネットワークシステムを提供することにある。

【０００７】また、本発明の目的は、前述の動的ポートを使用する多種多様な個別ＡＰのＶＰＮ構築を容易に実現することのできるネットワークシステムを提供することにある。

【０００８】

【課題を解決するための手段】本発明によれば前記目的は、ＡＰインタフェースに変更を加えずに前述した目的を達成するために、ＦＷにある特定のアクセス可能なポートを設け、また、そのポートを用いて許可されたＡＰのデータを転送する次の２つの手段を設けることにより達成される。すなわち、第１の手段は、ＦＷを挟み込む形で前記ポートを用いた通信路を確立し、この通信路を用いてＡＰデータを中継する中継手段であり、第２の手段は、ＡＰが動的ポートを使用するため通知する動的ポート通知を認識し、これを通知したＡＰのアクセス権限をチェックし、許されたＡＰならば、以後の動的ポートを用いたＡＰデータを前記中継手段を用いた通信に切り替える手段である。なお、前記中継手段に、ＡＰデータの暗号化を行う手段を設けるとよい。

【０００９】本発明は、前述の構成を備えることにより、中継手段がＦＷのアクセス可能ポートを用いてＡＰデータを転送するため、動的ポートを使用するＡＰを無改造で使用することができ、また、許可されたＡＰデータのみを中継手段を使用した通信に切り替えるようにすることにより、そのアクセスチェックも行うことが可能となる。

【００１０】また、前述の中継手段の通信路を暗号化することによりＦＷを介したＶＰＮを動的ポートを使用するＡＰにおいて実現することができる。

【００１１】本発明によれば前記目的は、具体的には、相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構成され、前記サーバ計算機と前記クライアント計算機上のＡＰとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記汎用アクセスチェック装置により保護されたネットワークと接続される第１のデータ通信手段と、前記汎用アクセスチェック装置で保護されていないネットワークに接続される第２のデータ通信手段と、前記第１と第２のデータ通信手段の相互間にデータ転送パスを構築する手段と、前記クライアント計算機上の特定ＡＰを変更することなく前記第２のデータ通信手段と通信を行って前記特定ＡＰのデータを転送する手段と、前記第１の通信手段と第２の通信手段との間のデータ転送パスを用いて前記特定ＡＰのデータを中継するデータ中継手段と、特定ＡＰのデータ内容に基づいて前記特定ＡＰのデータ中継手段を制御する手段とを備えることにより達成される。

【００１２】前述した本発明の目的を達成するための構成の種々の変形例は、発明の実施形態の説明において詳細に説明する。

【００１３】

【発明の実施の形態】以下、本発明によるネットワークシステムの実施形態を図面により詳細に説明する。

【００１４】図１は本発明の第１の実施形態によるネットワークシステムの構成例を示すブロック図であり、ＦＷを介してインターネットとイントラネットとを接続して構成されたネットワークシステムである。図１において、１００は内部セキュリティ代行サーバ(Ｉntra Ｓecurity Ｐroxy：以下、ＩＳＰという）、１０１は外部セキュリティ代行サーバ(Ｅxtra Ｓecurity Ｐroxy：以下、ＥＳＰという）、１０２はＦＷ、１０３はルータ（以下、Ｒという）、１０４はインターネットプロバイダ（以下、Ｐという）、１０５はクライアント計算機、１０６はサーバ計算機、１１０はイントラネット、１１１はインターネット、１１２は公衆電話網(Ｐablic Ｔelephone Ｎetwork：以下、ＰＴＮという）である。

【００１５】図１に示すように構成されるネットワークシステムにおいて、クラインアント計算機１０５ａ、１０５ｂ（両者を区別する必要のない場合、単に１０５と記す）は、ＰＴＮ１１２に接続されたＰ１０４、インターネット１１１、Ｒ１０３ａ、ＦＷ１０２、Ｒ１０３ｂを介してイントラネット１１０内のサーバ計算機１０６にアクセスする。クライアント計算機１０５からサーバ計算機１０６へのアクセスにおいて、ＦＷ１０２は、正当なアクセスのみを中継する。また、Ｒ１０３ａ、１０３ｂ（両者を区別する必要のない場合、単に１０３と記す）は、ネットワーク間を接続しデータパケットの振り分けを行う。図示ネットワークシステムは、イントラネット１１０へのアクセスに対する保護を強固なものとするため、各ネットワーク相互間をＦＷ１０２とＲ１０３とを介して接続する。

【００１６】ＦＷ１０２とインターネット側のＲ１０３ａとが接続されたセグメントには、ＥＳＰ１０１が接続されている。また、ＦＷ１０２の内側のセグメントには、ＩＳＰ１００が接続されている。ＩＳＰ１００とＥＳＰ１０１とは、両者で協力してＦＷ１０２の持つアクセスチェック機能を補完する。ＦＷ１０２、クライアント１０５、サーバ１０６、ＥＳＰ１０１、ＩＳＰ１００は、共にＣＰＵとメモリとからなるよく知られた計算機システムにより構成されている。

【００１７】図２はクライアント計算機１０５のソフトウエア構造を説明する図であり、以下、これについて説明する。

【００１８】図２において、２００はクライアント用Ａ

Ｐであり、種々の処理を行う通信プログラムである。クライアント用ＡＰは、具体的には、ファイル転送、テルネット、ネットワークチャット等、あるいは、その他の業務用処理を行うプログラムであり、ＯＳ２０３上で動作する。ＯＳ２０３は、通信プロトコルを制御してインターネット１１１上でのデータ送受信処理を担当するＴＣＰ／ＩＰ処理２０６とＰＴＮ１１２を介したＰ１０４とのデータ送受信処理を担当するＰＰＰ処理２０７とを含む。

【００１９】また、クライアント計算機１０５は、クライアント用ＡＰ２００とＴＣＰ／ＩＰ処理２０３とのインタフェースを処理するソケット処理２０２を含む。従来の処理では、クライアント用ＡＰ２００がソケット処理２０２を直接呼び出すが、本発明では、ソケット処理２０２とクライアント用ＡＰ２００との間にソケットフック処理２０１をミドルウエアとして設けている。また、本発明の第１の実施形態では、補助アプリケーションとして目的のＰ１０４との間でＰＰＰ処理２０７を起動させるプロバイダアクセス処理２０５を持ち、また、ＰＴＮ１１２上の伝送制御を行うモデムドライバ２０４を含む。

【００２０】ソケットフック処理２０１は、クライアント用ＡＰ２００とのインタフェースとしてソケット処理２０２と全く同一のインタフェースを提供し、かつ、ソケット処理２０２とのインタフェースを利用してクライアント用ＡＰ２００にソケットインタフェースを提供する。また、ソケットフック処理２０１は、認証・暗号・アクセス先制御機能を持つ。このソケットフック処理２０１により、クライアント用ＡＰは、無改造でＦＷ１０２を含むネットワークシステムに適応することができる。

【００２１】図３はＦＷ１０２のソフトウエア構造を説明する図であり、以下、これについて説明する。図３において、３００はＦＷメイン処理であり、ＦＷメイン処理３００は、中継処理３０１、認証処理３０２、ネゴシエーション処理３０３から構成される。また、ＦＷ１０２は、クライアント計算機１０５と同様にソケット処理２０２とＴＣＰ／ＩＰ処理２０３とを持つ。

【００２２】ＦＷメイン処理３００は、ＦＷ１０２のＡＰとして動作する。このＦＷ１０２は、サーキットゲートウェイ型であり、ネゴシエーション処理３０３で接続先や送信者のＩＤを送受し、認証処理３０２により確認した送信者からのデータを中継処理３０１がソケットレベルで中継する。この中継処理３０１は、データを暗号化して送るという機能を有していない。

【００２３】図４はＥＳＰ１０１のソフトウエア構成を説明する図であり、以下、これについて説明する。図４において、４０３はＥＳＰメイン処理であり、ＥＳＰメイン処理４０３は、ＩＳＰ１００との通信を行うＩＳＰプロトコル処理４００、クライアントとの通信を行うクライアントプロトコル処理４０１、データの中継を行う中継処理４０２から構成される。また、ＦＷ１０２と同様にソケット処理２０２とＴＣＰ／ＩＰ処理２０３とを持つ。

【００２４】図５はＩＳＰ１００のソフトウエア構成を説明する図であり、以下、これについて説明する。図５において、５００はＩＳＰメイン処理であり、ＩＳＰメイン処理５００は、ＥＳＰとの通信を行うＥＳＰプロトコル処理５０２、ＡＰデータ解析制御処理５０１、中継処理５０３から構成される。また、ＦＷ１０２やＥＳＰ１０１と同様にソケット処理２０２とＴＣＰ／ＩＰ処理２０３とを持つ。また、５０６はＩＳＰ１００のＯＳであり外部Ｉ／Ｏ装置との入出力を制御する。このＯＳ５０６は、設定情報５０５を変更するテキストエディタ５０４を備える。設定情報には、後に説明する各ＡＰ毎の動的アドレス通知を判定する条件がテキストとして記述されている。ＡＰデータ解析制御処理５０１は、前述の条件に基づいて動的アドレス通知の判定処理を実行する。

【００２５】前述したように、ＩＳＰ１００は、多様なＡＰへ対応する場合、テキストエディタ５０４を使用して設定情報を変更すればよいので、ＡＰＧＷ方式のＦＷを追加するより開発コストが少なくすみ、かつ、拡張性もよいという効果を得ることができる。

【００２６】図６は本発明の第１の実施形態による図１に示すネットワークシステムにおけるＥＳＰとＩＳＰとの間のプロトコルを説明するシーケンス図であり、図６を参照して、各装置における処理を詳細に説明する。

【００２７】（１）まず、ＩＳＰ１００とＥＳＰ１０１との間でＦＷ１０２を介した通信を行い、ＩＳＰ１００とＥＳＰ１０１との初期化を行い、論理的セッションを開設する。この後、クライアント１０５のＡＰ２００は、サーバ１０６とのコネクションを確立するためのconnect要求を発行する（ステップ６００、６０１）。

【００２８】（２）次に、クライアント用ＡＰ２００からのコネクト要求を受けたソケットフック処理２０１は、コネクション確立先をサーバ１０６からＥＳＰ１０１に換えてコネクションを確立する（ステップ６０２）。

【００２９】（３）クライアント１０５のソケットフック処理２０１からのコネクションを受諾したＥＳＰ１０１は、ＦＷ１０２の持つ認証機能を利用するため、ＦＷ１０２に対してコネクションを確立し、次に、クライアント認証を行うために必要な情報の中継処理を行う。このようにして、クライアント１０５の認証がＥＳＰ１０１を介してＦＷ１０２で行われる（ステップ６０３、６０５）。

【００３０】このように、本発明の実施形態によるＥＳＰ－ＩＳＰ間のプロトコルは、ＦＷ１０２の認証機能を利用しているため、ＥＳＰ１０１やＩＳＰ１００に認証

のためのデータベースを持つ必要がなく、認証情報を設定する必要がなく管理がしやすいという利点がある。

【００３１】（４）ステップ６０５の認証シーケンスの途中において、ＦＷ１０２は、クライアント１０５を確認すると、サーバ１０６とのコネクションを確立する（ステップ６０４）。

【００３２】（５）そして、ステップ６０５の最後にＦＷ１０２は、中継路が確立したことをクライアント１０５へ通知する。このＦＷ１０２の中継経路確立通知を受けたＥＳＰ１０１は、すぐにクライアント１０５への中継を行わず、以下に説明する一連の処理が終了するまで前記通知を保留する。次に、ＥＳＰ１０１は、ＦＷ１０２とのコネクションを解放することにより、ＦＷ１０２の中継路を解放する（ステップ６０６）。

【００３３】（６）次に、ＥＳＰ１０１は、一時的な暗号鍵を生成してクライアント１０５との間でこの暗号鍵を交換する（ステップ６０７）。

【００３４】このように、コネクション単位の暗号鍵を使用することにより暗号鍵の推定がしにくくなりセキュリティを高めることができる。また、ＦＷ１０２に暗号化機能が無くても、ＥＳＰ１０１が暗号化機能をＦＷ１０２の変更をせずに実現することができるという利点を持つ。

【００３５】（７）次に、ＥＳＰ１０１は、ＩＳＰ１００を介したサーバ１０６とのコネクション要求を、ステップ６００で先に確立したセッションを通じて送る。これを受けた、ＩＳＰ１００は、サーバ１０６とのコネクションを確立し、その応答をＥＳＰ１０１に返す（ステップ６０８～６１０）。

【００３６】（８）これを受けたＥＳＰ１０１は、保留しておいた中継路確立応答をクライアント１０５側に返す。このＥＳＰ１０１からの中継路確立応答を受けたソケットフック処理２０１は、ＡＰ２００に対して正常リターンすることにより、サーバ１０６とのコネクションが確立したことをＡＰ２００へ通知する（ステップ６１１、６１２）。

【００３７】前述した処理により、クライアント１０５とサーバ１０６との仮想的なコネクションが、ＩＳＰ１００、ＦＷ１０２、ＥＳＰ１０１の各コネクションを中継した形で実現できる。

【００３８】次に、前述の処理により確立したコネクションを通じてデータが送られる際のシーケンスについて説明する。

【００３９】（９）クライアント用ＡＰ２００は、データを送るときソケットフック処理２０１に対して送信データとコネクションとを指定したｓｅｎｄ要求を発行する。これを受けたソケットフック処理２０１は、ＥＳＰ１０１に対してＡＰ２００からのデータを送信する（ステップ６１３、６１４）。

【００４０】（10）クライアント１０５からのデータを受信したＥＳＰ１０１は、データをカプセル化してＩＳＰ１００へ渡す。このカプセル化されたデータを受けたＩＳＰ１００は、そのデータの内容をチェックし、クライアントによる通信アドレスの通知であるか否かを判定する（ステップ６１５、６１６）。

【００４１】（11）ステップ６１６のチェックで条件に合致しない場合、ＩＳＰ１００は、カプセル化されたデータを元のデータに戻し、ステップ６０９で確立したコネクションを用いてデータをサーバ１０６に渡す。ステップ６１６のチェックで条件が合致した場合、すなわち、クライアントによる通信アドレスの通知であった場合、ＩＳＰ１００は、ＥＳＰ１０１にクライアント１０５とのコネクション確立要求を送る（ステップ６１７、６１８）。

【００４２】（12）これを受けたＥＳＰ１０１は、クライアント１０５とのコネクションを確立する。このときコネクションの受け入れ待ちとなるクライアント用ＡＰ２００は、ａｃｃｅｐｔ要求をソケットフック処理２０１に対して要求しておく。そして、ソケットフック処理でステップ６１９によるＥＳＰ１０１とのコネクションが確立したら、ソケットフック処理２０１は、そのことをＡＰ２００にリターンにより通知する（ステップ６１９～６２１）。

【００４３】（13）クライアント１０５とのコネクションを確立したＥＳＰ１０１は、その結果をＩＳＰ１００に通知する。このコネクション確立通知を受けたＩＳＰ１００は、ステップ６１６で保留した中継ＡＰデータ中のクライアントの通信アドレスをＩＳＰ１００自身の通信アドレスに変えてサーバ１０６に送る（ステップ６２２、６２３）。

【００４４】（14）ＩＳＰ１００から通信アドレスを受けたサーバ１０６は、ＩＳＰ１００の通信アドレス宛にコネクションを張り、これにより確立したコネクションを用いてデータを転送する（ステップ６２４、６２５）。

【００４５】（15）これを受けたＩＳＰ１００は、データをＥＳＰ１０１へ中継する。このサーバ１０６からのデータを受けたＥＳＰ１０１は、クライアント１０５にステップ６１９で確立したコネクションを用いてそのデータを中継する。クライアント用ＡＰ２００は、データを受け取るためｒｅｃｖ要求を発行しておき、その応答としてデータを受け取る（ステップ６２６～６２９）。

【００４６】前述したシーケンスを処理するＩＳＰ１００とＥＳＰ１０１、及び、クライアント１０５のソケットフック処理２０１により、ＳＣＧＷタイプのＦＷ１０２を介して接続されるクライアント１０５とサーバ１０６とにおいて、クライアント用ＡＰ２００が、サーバ１０６に対して動的に割り当てられたクライアント用ＡＰ２００の通信アドレスを通知し、これを受けたサーバ１０６から通知されたクライアント通信アドレス宛にデー

タを送信する処理を行うアプリケーションプログラムのアクセスチェックを当該アプリケーションを改造することなく実現することができる。

【００４７】図７は図６により説明したＩＳＰ１００とＥＳＰ１０１との間の通信プロトコルメッセージのフォーマットを説明する図である。

【００４８】図７において、７００は共通フォーマットであり、この共通フォーマット７００は、コマンドフィールド７０１、コネクションＩＤフィールド７０２、コマンド個別フィールド７０３の３つのフィールドから構成される。そして、コマンド個別フィールド７０３のみ可変長であり、その他のフィールドは固定長であり、コマンドフィールド７０１内の値によって各種メッセージが判別できる。

【００４９】７１０はコマンドフィールド７０１内の値とその名称を示した表である。各コマンドには、次の５種類がある。すなわち、ステップ６０８に対応するｉｎｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｅｑ、ステップ６１０に対応するｉｎｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｓｐ、ステップ６１５と６２６に対応するｄａｔａ－ｔｒａｎｓｆｅｒ．ｒｅｑ、ステップ６１８に対応するｏｕｔｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｅｑ、ステップ６２２に対応するｏｕｔｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｓｐの５つである。

【００５０】また、７２０は前述の各コマンドにおけるコネクションＩＤフィールド７０２の内容を示した表である。この表７２０におけるｏｕｔｓｉｄｅ－ｃｏｎｎｅｃｔｉｎ　ＩＤは、ＥＳＰ１０１がシーケンスのステップ６０２で確立するクライアント１０５とのコネクションを識別する番号である。また、ｉｎｓｉｄｅ－ｃｏｎｎｅｃｔｉｎ　ＩＤは、ＩＳＰ１００がシーケンスのステップ６２４で確立するサーバ１０６とのコネクションを識別する番号である。

【００５１】７３０は前述の各コマンドにおけるコマンド個別フィールド７０３の内容を示した表である。この表７３０におけるｉｎｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｅｑのｓｅｒｖｅｒ　ａｄｄｒｅｓｓは、サーバ１０６の通信アドレスである。また、ｉｎｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｓｐのｒｅｓｕｌｔ　ｃｏｄｅは、ステップ６０９の結果を示す値であり、ｄａｔａ－ｔｒａｎｓｆｅｒ．ｒｅｑのＡＰｐｌｉｃａｔｉｏｎ　ｄａｔａは、サーバ１０６とクライアント１０５との間で転送される通信データである。さらに、ｏｕｔｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｅｑのｃｌｉｅｎｔ　ａｄｄｒｅｓｓは、ステップ６１６のチェックで該当するデータをサーバ１０６へ送ったクライアント１０５の通信アドレスであり、ｏｕｔｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｓｐのｒｅｓｕｌｔ　ｃｏｄｅは、ステップ６１９で確立されるＥＳＰ１０１とクライアント１０５とのコネクションの結果である。また、ｎｅｗ　ｏｕｔｓｉｄｅ－ｃｏｎｎｅｃｔｉｏｎ　ＩＤは、ステップ６１９で確立されるＥＳＰ１０１とクライアント１０５との間のコネクションを識別する番号である。

【００５２】図８はＩＳＰ１００とＥＳＰ１０１との間の初期化用セッション確立の処理を説明するシーケンス図であり、次に、前述したＦＷ１０２を介して張られるＩＳＰ１００とＥＳＰ１０１との間の初期化用セッション確立ステップ６００の処理の詳細を図８を参照して説明する。

【００５３】（１）まず、初期化用セッションの確立の要求は、ＩＳＰ１００側から行われる。このため、ＩＳＰ１００は、ＦＷ１０２に対してコネクションを確立し、ＦＷ１０２に対してＥＳＰ１０１との接続要求としてｃｏｎｎｅｃｔ．ｒｅｑを発行する（ステップ８００、８０１）。

【００５４】（２）ｃｏｎｎｅｃｔ．ｒｅｑを受けたＦＷ１０２のメイン処理３００は、接続先であるＥＳＰ１０１とコネクション確立する。そして、メイン処理３００は、ＩＳＰ１００へ接続完了応答ｃｏｎｎｅｃｔ．ｒｓｐを返す（ステップ８０２、８０３）。

【００５５】この接続完了応答ｃｏｎｎｅｃｔ．ｒｓｐをＩＳＰ１００が受け取ることにより、ＦＷ１０２を介したＩＳＰ１００とＥＳＰ１０１との間のセッションが確立される。前述の処理を終了したＦＷ１０２は、以後データの中継だけを行う。前述した本発明の実施形態による処理は、ＦＷ１０２によるＩＳＰ１００の認証処理を行わず、ＥＳＰ１０１がＩＳＰ１００の認証を行っている。

【００５６】（３）次に、ＩＳＰ１００は、ｔｒｉａｌ．ｒｅｑをＥＳＰ１０１宛に送る。このｔｒｉａｌ．ｒｅｑには、乱数とその乱数をＩＳＰ１００及びＥＳＰ１０１間の共通鍵で暗号化した値とが含まれており、これらがペアで送られる（ステップ８０４）。

【００５７】（４）ｔｒｉａｌ．ｒｅｑを受けたＥＳＰ１０１のメイン処理４００は、送られた暗号化乱数を手持ちの共通鍵により解読し、解読した値が送られた乱数と一致したことによりＩＳＰ１００を確認する。そして、同様に乱数と暗号化した乱数とのペアをｔｒｉａｌ．ｒｓｐとしてＩＳＰメイン処理５００に送る（ステップ８０５）。

【００５８】（５）これを受けたＩＳＰ１００のメイン処理５００は、先に述べたと同様の方法でＥＳＰ１０１の認証を行う。次に、ＩＳＰメイン処理５００は、初期化データをＥＳＰ１０１へ送る（ステップ８０６）。

【００５９】図９は前述した本発明の第１の実施形態におけるＥＳＰとＩＳＰとの間の初期化処理のロジックとＦＷ処理のロジックとを説明するフローチャートである。９３００はＦＷメイン処理３００の処理フローであり、まず、これによりＦＷ１０２の処理を説明する。

【００６０】（１）ＦＷ１０２は、コネクションを中継

するタイプのＦＷである。このため、ＦＷ１０２は、まず、ａｃｃｅｐｔ要求によりコネクションの受け付けを行い、次に、確立されたコネクションにより相手からの中継要求を受信する（ステップ９３１０、９３２０）。

（２）次に、中継要求を送った相手の認証が必要か否かをチェックし、この結果、認証が必要であれば、認証処理を行う（ステップ９３３０、９３４０）。

（３）次に、中継要求に記載された接続相手へのコネクションを要求を出し、中継先コネクションを確立する（ステップ９３５０）。

（４）次に、ステップ９３１０で確立したコネクションとステップ９３５０で確立したコネクションとからのデータを相互に中継するため、これらコネクションを対応させる。そして、このようにして確立された中継路の確立完了応答を中継要求の送り主に対して返送する（ステップ９３６０）。

（５）そして、対応させたコネクション間でのデータの中継処理を行う（ステップ９３７０）。

【００６１】９５００はＩＳＰメイン処理５００によるＥＳＰ１０１とＩＳＰ１００との間の初期化処理ロジックの処理フローであり、以下、これについて説明する。

【００６２】（１）まず、ＩＳＰメイン処理５００は、ＦＷ１０２とのコネクションを確立し、ＦＷ１０２に対してＥＳＰ１０１との中継要求を発行する（ステップ９５１０、９５２０）。

（２）次にＩＳＰメイン処理５００は、ＥＳＰ１０１との間で認証を経ることにより登録を実行し、初期データをＥＳＰ１０１へ送付する（ステップ９５３０、９５４０）。

【００６３】９４００はＥＳＰメイン処理４００によるＥＳＰ１０１とＩＳＰ１００との間の初期化処理ロジックの処理フローであり、以下、これについて説明する。

【００６４】（１）まず、ＥＳＰメイン処理４００は、ＦＷ１０２を介してＩＳＰ１００からのコネクションを受け付ける（ステップ９４１０）。

（２）次に、ＥＳＰメイン処理４００は、ＩＳＰ１０１の認証を行い、当該ＩＳＰ１０１を記憶し、ＩＳＰ１００からの初期データを受信する（ステップ９４２０、９４３０）。

【００６５】図１０は前述した本発明の実施形態におけるサーバ１０６とクライアント１０５上のそれぞれのアプリケーションプログラムの処理ロジックのフローチャートであり、図１０を参照してクライアント用ＡＰ２００とサーバ用ＡＰ２０００との処理を説明する。

【００６６】まず、クライアント用ＡＰ２００の処理を説明する。

（１）まず、サーバ１０６と制御コネクションを確立し、次に、ユーザからのコマンドを受け付けて、転送要求か否かのチェックを行い、転送要求でなければ、当該コマンドの処理を行う（ステップ１０１０～１０３０）。

（２）ユーザからのコマンドが転送要求であれば、サーバ１０６に制御コネクションによりデータ転送要求を通知し、自分の通信アドレスである通信ポートをＴＣＰ／ＩＰ処理２０３に依頼することにより、通信ポートを動的に割り当ててもらう（ステップ１０４０、１０５０）。

（３）そして、割り当てられた通信ポートをサーバ１０６に通知し、サーバ１０６からの転送用コネクションを受け付ける（ステップ１０６０、１０７０）。

（４）次に、ステップ１０７０の処理で確立した転送コネクションを用いてデータ転送を行う。その後、ステップ１０２０のユーザコマンドの受け付けの処理に戻る（ステップ１０８０）。

【００６７】次に、サーバ用ＡＰ２０００の処理フローを説明する。

（１）まず、クライアント１０５からのコネクションを受け付け、クライアントからの要求を受信する（ステップ２０１０、２０２０）。

（２）次に、クライアントから受信した要求がデータ転送要求であるか否かを判別し、転送要求でなければ、要求に応じた処理を行う（ステップ２０４０、２０３０）。

（３）受信した要求が転送要求であれば、クライアントＡＰ２００からのポート通知を受信するまで待つ（ステップ２０５０）。

（４）次に、通知されたクライアントＡＰ２００のポート宛にコネクション要求を出すことにより転送コネクションを確立させ、確立した転送コネクションによりデータの転送を行う（ステップ２０６０、２０７０）。

【００６８】図１１は本発明の第１の実施形態におけるクライアント１０５上のソケットフック処理２０１の動作を説明するフローチャートであり、以下、これについて説明する。

【００６９】（１）まず、ソケットフック処理２０１は、クライアント用ＡＰ２００からの通信コマンドを受け取り、各コマンド毎に処理の振り分けを行う（ステップ１１００）。

（２）通信コマンドがｃｏｎｎｅｃｔコマンドであった場合、まず、ＥＳＰ１０１とコネクションを確立し、確立されたＥＳＰ１０１とのコネクションを用いてＦＷ１０２に対して、サーバ１０６への中継接続を要求する（ステップ１１１０、１１１２）。

（３）次に、ＦＷ１０２による認証処理を行い、ＥＳＰ１０１と暗号鍵を交換する（ステップ１１１４、１１１６）。

（４）次に、ＥＳＰ１０１を経由したＦＷ１０２からの中継接続応答を受信し、リターンすることによりＡＰに応答を返す（ステップ１１１８、１１６０）。

【００７０】（５）通信コマンドがａｃｃｅｐｔコマン

ドであった場合、まず、ＥＳＰ１０１からのコネクションを受け付けて、ＥＳＰ１０１と鍵交換を行い、その後、リターンすることによりＡＰに応答を返す（ステップ１１２０、１１２２、１１６０）。

【００７１】（６）通信コマンドがｓｅｎｄコマンドであった場合、まず、データの暗号化を行い、ソケット処理２０２にコマンドを渡す。そして、ソケット処理２０２からのリターンをリターンすることによりＡＰに応答を返す（ステップ１１３０、１１５０、１１６０）。

【００７２】（７）通信コマンドがｒｅｃｖコマンドであった場合、まず、ソケット処理２０２にコマンドを渡し、受信データの解読を行う。そして、リターンすることによりＡＰに応答を返す（ステップ１１４０、１１４２、１１６０）。

【００７３】（８）通信コマンドが前述以外のコマンドの場合、ソケット処理２０２にコマンドを渡し、ソケット処理２０２からのリターンをリターンすることによりＡＰに応答を返す（ステップ１１５０、１１６０）。

【００７４】図１２は本発明の実施形態におけるＩＳＰメイン処理３００の処理を説明するフローチャートであり、以下、これについて説明する。

【００７５】（１）まず、ＩＳＰ１００は、図９及び図８により説明したように、ＥＳＰ１０１とのセッションを開設し、次に、ＥＳＰ１０１からのコマンドを受信して、そのコマンドが接続要求（ｉｎｓｉｄｅ－ｃｏｎｎｅｃｔ．ｒｅｑ）であるか否かを判断し、接続要求でなければ接続要求の受信待ちとなる（ステップ１２００、１２０２）。

【００７６】（２）ステップ１２０２で接続要求が受信されると、次に、サーバ１０６とのコネクションを確立し、次に、ＥＳＰ１０１にサーバ１０６とのコネクションが確立したことを通知する（ステップ１２０４、１２０６）。

【００７７】（３）次に、データを受信し、中継処理を行う。このとき、サーバ１０６とのコネクションから受けたデータにＩＳＰ－ＥＳＰプロトコルヘッダを付け、これをＥＳＰセッションでＥＳＰ側へ転送する中継処理を行う（ステップ１２０８、１２１０）。

【００７８】（４）他方、ＥＳＰセッションから受信したデータは、そのデータ内容が判定される。それが通信アドレス通知でなければ、そのデータをサーバ１０６へ中継し、ステップ１２０８の処理に戻る（ステップ１２１２、１２１４）。

【００７９】（５）ステップ１２１２で判定したデータ内容が通信アドレス通知であれば、ＥＳＰ１０６宛に、クライアントとのコネクションを確立する要求を出し、次に、ＥＳＰ１０６からのクライアントとのコネクションが確立したという確認応答を受信する（ステップ１２１６、１２１８）。

【００８０】（６）次に、データ内容の通信アドレスを自分自信の通信アドレスに書き換えてデータの中継を行い、サーバからのコネクションを受け付けた後、ステップ１２０８の処理に戻る（ステップ１２２０、１２２２）。

【００８１】図１３は本発明の実施形態におけるＥＳＰメイン処理４００の処理動作を説明するフローチャートであり、以下、これについて説明する。

【００８２】（１）まず、ＥＳＰ１０１は、図９及び図８により説明したように、ＩＳＰ１００とのセッションを開設し、次に、クライアント１０５からのコネクションを受け付けるまで待つ（ステップ１３００、１３０２）。

【００８３】（２）次に、ＦＷ１０２とのコネクションを確立して、ＦＷ１０２への認証データの中継を行い、ＦＷ１０２からの応答を受信する。その後、ＦＷ１０２とのコネクションを切断する（１３０４～１３１０）。

【００８４】（３）次に、暗号鍵を生成してクライアントと交換し、サーバ１０６とのコネクションの要求をＩＳＰ１００に送る。そして、ＩＳＰ１００からのサーバ１０６とのコネクションが確立したことを示す応答メッセージを受信し、クライアント１０５へコネクション確立応答を送信する（ステップ１３１２～１３１８）。

【００８５】（４）次に、データの受信を行い内容で処理を振り分ける。そして、受信したデータが中継用のデータであれば、その受信データの中継を行って、データ受信のステップ１３２０に戻る。このとき、データのデータの暗号化・解読を行う（ステップ１３２０、１３２２）。

【００８６】（５）ステップ１３２０で受信したデータがクライアントとのコネクション確立要求のデータであった場合、クライアント１０５とのコネクションを確立し、暗号鍵をクライアン１０５と交換する。そして、クライアント１０５とのコネクション確立応答をＩＳＰ１００に送信し、ステップ１３２０の処理に戻る（ステップ１３２４～１３２８）。

【００８７】図１４は本発明の第２の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図１の場合と同一である。

【００８８】前述までに説明した本発明の第１の実施形態は、ＦＷ１０２を介してＩＳＰ１００とＥＳＰ１０１との間で通信を行う例であったが、図１４に示す本発明の第２の実施形態は、ＩＳＰとＥＳＰとの間を直接接続する通信路１４００（例えば、ＬＡＮ接続）を設け、通信路１４００を用いてＩＳＰとＥＳＰとの間のセッションを確立し、初期化データや中継データを流すものである。

【００８９】この本発明の第２の実施形態は、クライアント１０５のソケットフック処理２０１がＦＷ１０２と接続するものとＥＳＰ１０１と接続するものとを通信相手のアドレスにより振り分ける機能を持つ。このような

構成とすることにより、ＦＷ１０２の負荷を軽減することができるという効果得ることができる。

【００９０】図１５は本発明の第３の実施形態によるネットワークシステムの構成例の一部を示すブロック図である。図１５において、１５００は計算機装置であり、他の符号は図１の場合と同一である。

【００９１】前述した本発明の第１、第２の実施形態は、ＩＳＰ１００とＥＳＰ１０１とを独立した計算機システムで実現した例であったが、図１５に示す本発明の第３の実施形態は、１つの計算機装置１５００内でＩＳＰメイン処理５００とＥＳＰメイン処理４００とを動作させるようにしたものである。そして、ＩＳＰメイン処理５００とＥＳＰメイン処理４００とは、ＦＷ１０２の内側と外側とのネットワークに接続されており、また、ＩＳＰメイン処理５００とＥＳＰメイン処理４００とは、プロセス間通信を行う。

【００９２】前述のように、同一の計算機装置１５００上にＩＳＰメイン処理５００とＥＳＰメイン処理４００と実現することにより、動的通信アドレスを使用するＡＰをサポートするときの導入コストを抑えることができる。また、前述した本発明の第２の実施形態の場合と同様に、クライアント１０５のソケットフック処理２０１に、ＦＷ１０２と接続するものとＥＳＰ１０１と接続するものとを通信相手のアドレスにより振り分ける機能を持たせることにより、ＦＷ１０２の負荷を軽減することができるという効果を得ることができる。

【００９３】図１６は本発明の第４の実施形態によるネットワークシステムの構成例の一部を示すブロック図であり、図の符号は図１の場合と同一である。

【００９４】この本発明の第４の実施形態は、前述した本発明の第１の実施形態におけるＦＷ１０２の上でＩＳＰメイン処理５００とＥＳＰメイン処理４００とＦＷメイン処理３００とが動作するようにしたものである。そして、ＩＳＰメイン処理５００とＥＳＰメイン処理４００とＦＷメイン処理３００とは、それぞれプロセス間通信を行うことによりデータの中継を実行する。

【００９５】前述したように構成される本発明の第４の実施形態は、第３の実施形態よりも動的通信アドレスを使用するＡＰをサポートするときの導入コストを抑えることができる。

【００９６】図１７は本発明の第５の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図１の場合と同一である。

【００９７】この本発明の第５の実施形態は、前述した本発明の第１の実施形態におけるサーバ１０６内に、デーモンプロセスとしてＩＳＰメイン処理５００を実現するように構成したものであり、このような構成の実施形態においても、動的通信アドレスを使用するＡＰをサポートする場合の導入コストを抑えることができる。

【００９８】図１８は本発明の第６の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図１の場合と同一である。

【００９９】図１８に示す本発明の第６の実施形態は、ＥＳＰをインターネット上のサーバとして実現したものであり、プロバイダＩＳＰ１００とＥＳＰ１０１とを１対１のペアで存在させるのではなく、１つのＥＳＰ１０１に対して複数のＩＳＰ１００がセッションを確立してデータの中継を行うことを可能にしたものである。

【０１００】この実施形態によれば、ＥＳＰ１００を１つだけ設ければよいので、動的通信アドレスを使用するＡＰをサポートする場合の導入コストを抑えることができる。

【０１０１】図１９は本発明の第７の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図１の場合と同一である。

【０１０２】図１９に示す本発明の第７の実施形態は、前述した本発明の第１の実施形態におけるインタネットプロバイダ１０４内に、ＥＳＰ１０１を１つの装置として実現したものである。そして、この実施形態においては、１つのＩＳＰ１００に対して複数のＥＳＰ１０１がセッションを確立することができる。また、複数のＩＳＰ１００に対して複数のＥＳＰ１０１が、多対多のセッションを確立することもできる。

【０１０３】前述のように構成される本発明の第７の実施形態によれば、サービスプロバイダのサービスとして動的通信アドレスを使用するＡＰをサポートしていることをアピールすることができる。

【０１０４】図２０は本発明の第８の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図１の場合と同一である。

【０１０５】図２０に示す本発明の第８の実施形態は、前述した本発明の第１の実施形態におけるクライアント計算機１０５上にＥＳＰ１０１の機能を設けて構成したものであり、ＥＳＰメイン処理５００を動作させソケットフック処理２０１で行うコネクション確立先アドレスをＥＳＰメイン処理５００の内部アドレスにすることで容易に実現することができる。また、このとき、ＥＳＰとＩＳＰとの間のセッションの確立は、ＥＳＰ１０１の側から起動をかけることにより行うことができる。

【０１０６】前述の本発明の第８の実施形態によっても、動的通信アドレスを使用するＡＰをサポートする場合の導入コストを抑えることができる。

【０１０７】図２１は本発明の第９の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図１の場合と同一である。

【０１０８】図２１に示す本発明の第９の実施形態は、ＩＳＰメイン処理４００をサーバ計算機１０６上に、ＥＳＰメイン処理をクライアント計算機１０５上に設け、さらに、パケットフィルタ機能をもつルータ１０３を備えて実現したものである。また、この実施形態におい

て、ＥＳＰとＩＳＰとの各機能をエンド計算機に持たせることも可能である。このとき、ＩＳＰとＥＳＰとの間の認証機能を利用することにより、ＦＷ１０２は認証機能を持つことが不要である。

【０１０９】前述の実施形態は、サーキットゲートウエイタイプのＦＷでなくパケットフィルタ型のＦＷにも適用することができる。

【０１１０】前述までに説明した本発明の各実施形態は、図6により説明したと同等な固定的なシーケンスしか実行することができないものであった。しかし、本発明は、より複雑な動的通信アドレスを使用したＡＰのサポートも行うようにすることができる。いか、その例を説明する。

【０１１１】図２２はＩＳＰ１００が入力するＡＰ個別対応のアクセス制御マクロ言語の一例を示す図である。

【０１１２】図２２において、initial service-address は、サーバアプリケーションのよく知られた通信サービスアドレスが記述される。ＩＳＰ part は、ＩＳＰ１００におけるデータ内容のチェック条件と条件が一致したときの処理とをＩＳＰ－ＥＳＰプロトコルを含めてマクロ記述したものである。また、ＥＳＰ part も同様である。

【０１１３】ＩＳＰ１００は、前述のようなマクロに合わせてＡＰデータ解析処理５０１やＥＳＰプロトコル処理５０２を拡張する機能と、ＥＳＰ１０１に対する初期化データを生成する機能を持つ。ＥＳＰ１０１は、ＩＳＰ１００から送られたデータに基づいてＩＳＰプロトコル処理４０３を拡張する機能を持つ。なお、ＩＳＰ１００が、ＥＳＰ１０１で実行可能なオブジェクトを送付して、ＥＳＰ１０１がこれを実行するような形態をとってもよい。

【０１１４】前述により、より複雑な動的通信アドレスを使用したＡＰのサポートを容易に行うことが可能になる。また、複数のＥＳＰ１０１を接続するＩＳＰ１００は、それぞれのＥＳＰ１０１におけるアクセス制御ポリシーを別個に指定することができ、その設定を一括して行うことができるため、拡張性を含めて運用管理しやすいものとすることができる。

【０１１５】前述した本発明の各実施形態は、ＩＳＰ１００がデータをチェックするとして説明したが、本発明は、ＥＳＰ１０１側でデータチェックするようにすることも容易に実現できる。また、この実現においては、図２２で説明したように、ユーザがそのチェック条件を指定するようにすればよい。これにより、不要なデータをＩＳＰ１０１が受け取ることがないため、安全性を高めることができ、かつ、ＩＳＰ１００の負荷も軽減することができる。

【０１１６】図２３は本発明の第１０の実施形態によるネットワークシステムの構成例を示すブロック図である。

【０１１７】前述までに説明した本発明の各実施形態は、ＥＳＰ１０１をインターネット１１１の側に接続した例であったが、図２３に示す本発明の第１０の実施形態は、ＥＳＰ１０１を他のイントラネット１１０ｂに設けて構成したものである。すなわち、図２３に示す実施形態は、２つのイントラネット１１０ａ、１１０ｂを設け、一方のイントラネット１１０ｂの側にＥＳＰ１０１を設けたものである。

【０１１８】図２３に示す実施形態は、前述の構成を備えることにより、他のイントラネット内のクライアント１０５と自イントラネット内のサーバ１０６との間で通信を行うことができ、サーバを異なるイントラネットに移動させても通信を行うことができるという効果を得ることができる。

【０１１９】

【発明の効果】以上説明したように本発明によれば、以下に説明するような効果を得ることができる。

【０１２０】１．既存のＦＷを使用したネットワーク環境で、動的通信ポートを使用するＡＰを、そのＡＰを改造することなく使用して、ＦＷを介した安全な通信を行うことが可能となる。

【０１２１】２．また、ＦＷが暗号をサポートしている環境で、動的通信ポートを使用するＡＰを、そのＡＰを改造することなく適応させることができる。

【０１２２】３．同様に、ＦＷで認証機能をサポートした環境で、動的通信ポートを使用するＡＰを、そのＡＰを改造することなく適応させることができる。

【０１２３】４．また、ＦＷで暗号をサポートしない環境で、動的通信ポートを使用するＡＰを、ＡＰを改造することなく適応させることができ、かつ、暗号化をサポートすることも可能となる。

【０１２４】５．さらに、既存のＦＷを使用したネットワーク環境で、動的通信ポートを使用する複数のＡＰを、それらのＡＰを改造することなくサポートしたとき、各ＡＰのアクセス制御情報を纏めて作成し、各装置に反映させることができるため管理や運用を行いやすい。

【０１２５】６．また、前記５のアクセス制御情報の反映時、反映するデータが暗号化されているため、管理や運用のセキュリティを確保することができる。

【０１２６】７．また、本発明は、認証機能をサポートしているので、確実な相手とのみデータ転送を行うことができセキュリティを高めることができる。

【０１２７】８．また、ＦＷを仲介しないデータ転送路を確保した本発明は、ＦＷの負荷を軽減しネットワーク性能の向上を図ることができる。

【０１２８】９．また、異なるイントラネットを介して特定のＡＰを使用して通信を行うことができる。

【０１２９】１０．また、自社製業務用ＡＰを使用してインターネットからＦＷで区切られた自社イントラネッ

ト内のサーバと通信するとき、自社製のＡＰ用のＡＰＧＷを作成する必要がなく、その構築コストを抑えることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図２】図１におけるクライアント計算機のソフトウエア構造を説明する図である。

【図３】図１におけるＦＷのソフトウエア構造を説明する図である。

【図４】図１におけるＥＳＰのソフトウエア構成を説明する図である。

【図５】図１におけるＩＳＰのソフトウエア構成を説明する図である。

【図６】本発明の第１の実施形態によるネットワークシステムにおけるＥＳＰとＩＳＰとの間のプロトコルを説明するシーケンス図である。

【図７】図６により説明したＩＳＰとＥＳＰとの間の通信プロトコルメッセージのフォーマットを説明する図である。

【図８】ＩＳＰとＥＳＰとの間の初期化用セッション確立の処理を説明するシーケンス図である。

【図９】前述した本発明の第１の実施形態におけるＥＳＰとＩＳＰとの間の初期化処理のロジックとＦＷ処理のロジックとを説明するフローチャートである。

【図１０】前述した本発明の実施形態におけるサーバとクライアント上のそれぞれのアプリケーションプログラムの処理ロジックのフローチャートである。

【図１１】本発明の第１の実施形態におけるクライアント上のソケットフック処理２０１の動作を説明するフローチャートである。

【図１２】本発明の実施形態におけるＩＳＰメイン処理３００の処理を説明するフローチャートである。

【図１３】本発明の実施形態におけるＥＳＰメイン処理４００の処理動作を説明するフローチャートである。

【図１４】本発明の第２の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図１５】本発明の第３の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図１６】本発明の第４の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図１７】本発明の第５の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図１８】本発明の第６の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図１９】本発明の第７の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図２０】本発明の第８の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図２１】本発明の第２の実施形態によるネットワークシステムの構成例を示すブロック図である。

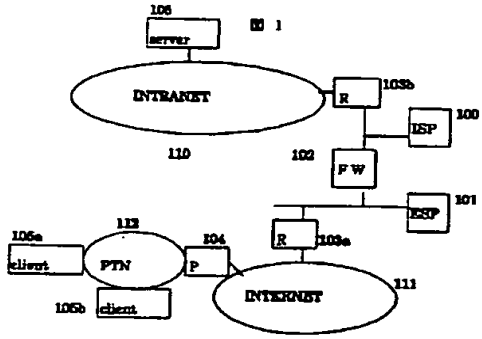
【図２２】ＩＳＰ１００が入力するＡＰ個別対応のアクセス制御マクロ言語の一例を示す図である。

【図２３】本発明の第１０の実施形態によるネットワークシステムの構成例を示すブロック図である。

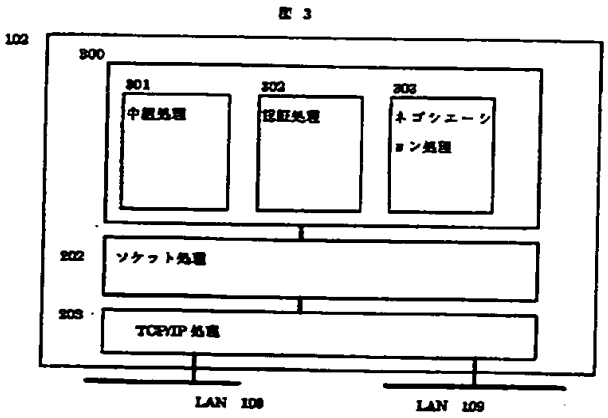
【符号の説明】

１００　内部セキュリティ代行サーバ（ＩＳＰ）
１０１　外部セキュリティ代行サーバ（ＥＳＰ）
１０２　ファイアウオール（ＦＷ）
１０３　ルータ（Ｒ）
１０４　インターネットプロバイダ（Ｐ）
１０５　クライアント計算機
１０６　サーバ計算機
１１０　イントラネット
１１１　インターネット
１１２　公衆電話網（ＰＴＮ）

【図１】

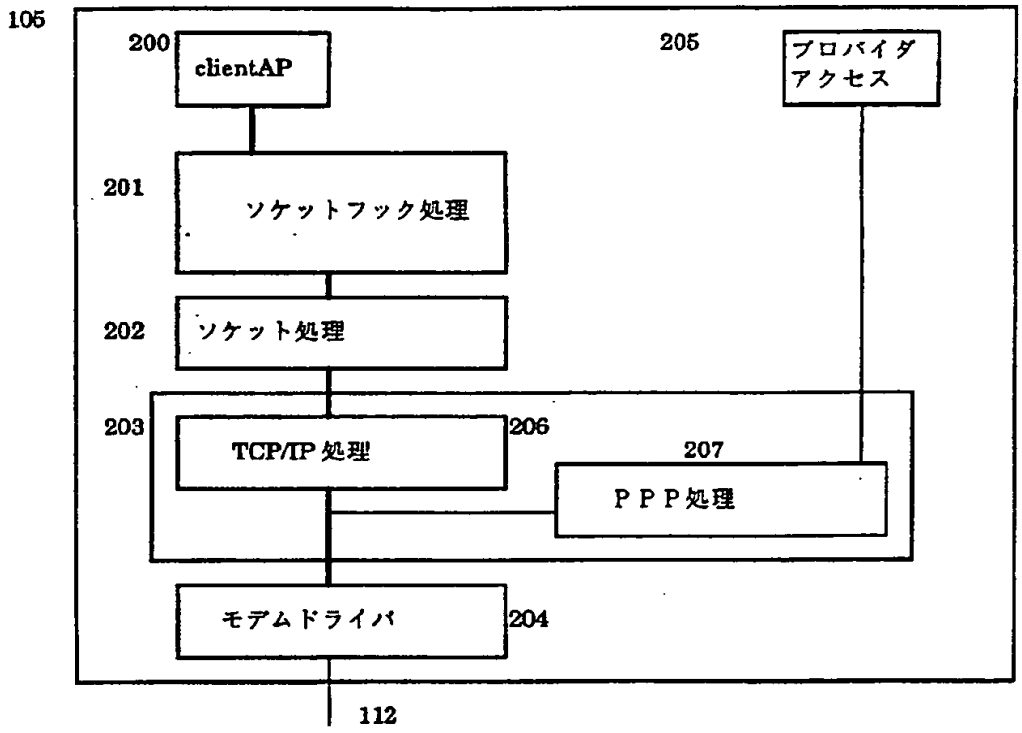


【図３】



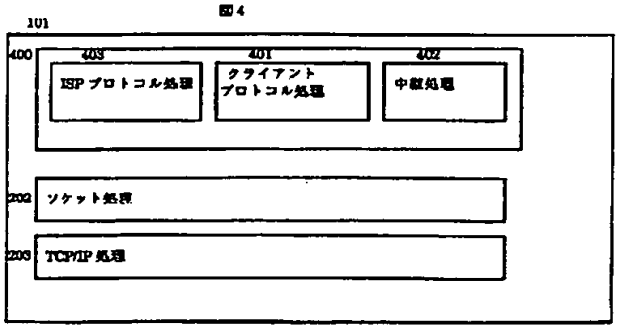
【図２】

図２



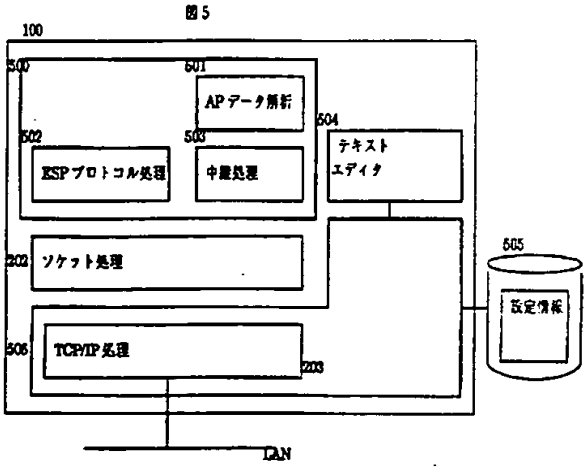
【図４】

図４



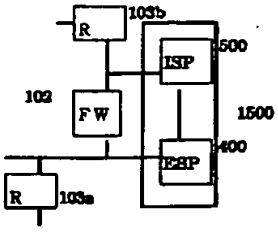
【図５】

図５



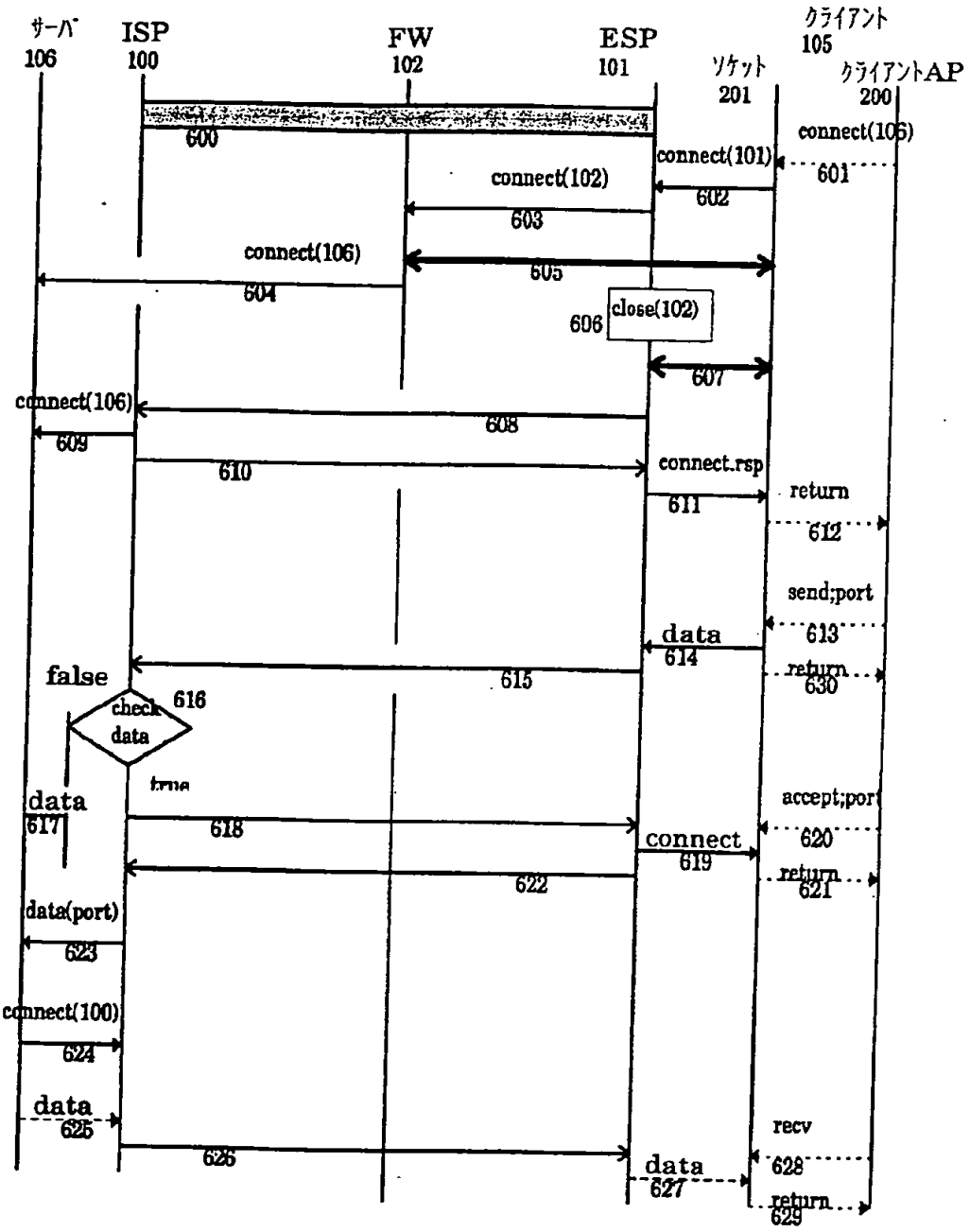
【図１５】

図 15



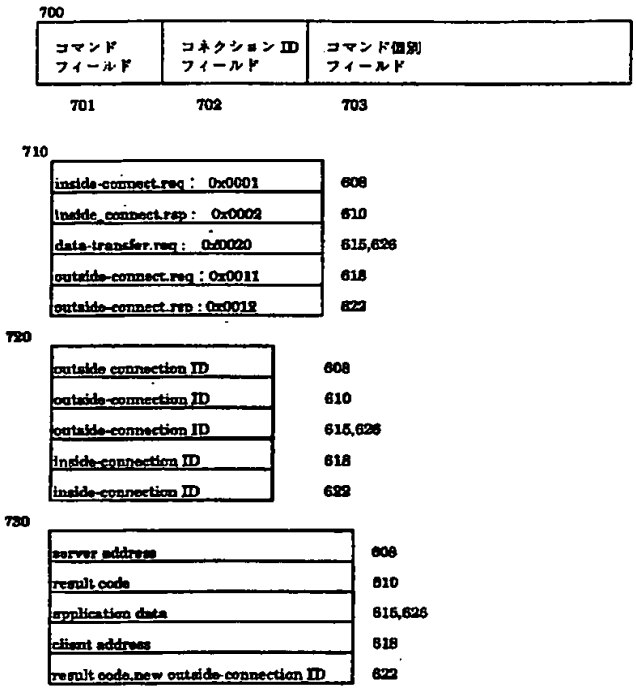
【図６】

図 6


サーバ
106
ISP
100
FW
102
ESP
101
ソケット
201
クライアント
105
クライアントAP
200
600
connect(106)
601
connect(101)
602
connect(102)
603
connect(106)
604
605
close(102)
606
607
connect(106)
608
609
610
connect.rsp
611
return
612
send;port
613
data
614
615
return
630
false
check data
616
true
data
617
618
accept;port
620
connect
619
return
621
622
data(port)
623
connect(100)
624
data
625
626
recv
628
data
627
return
629

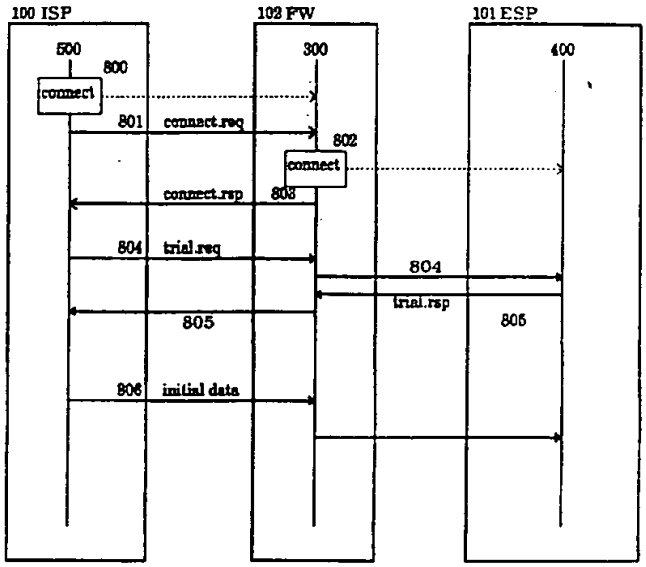
【図７】

図 7



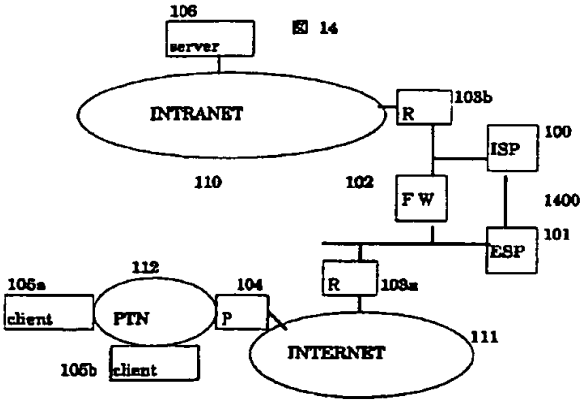
【図８】

図 8



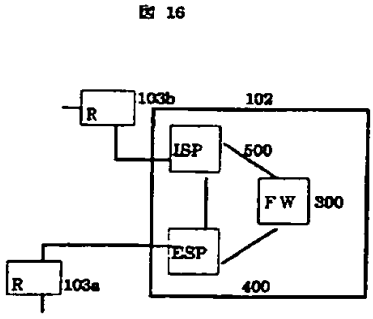
【図１４】

図 14



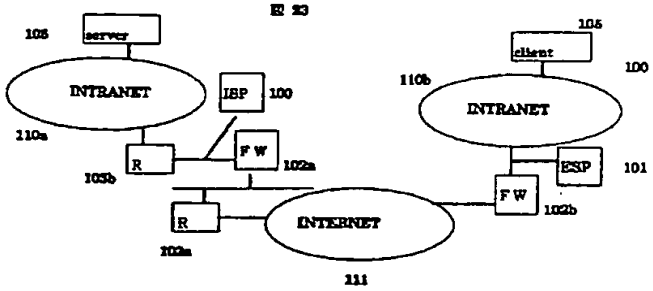
【図１６】

図 16



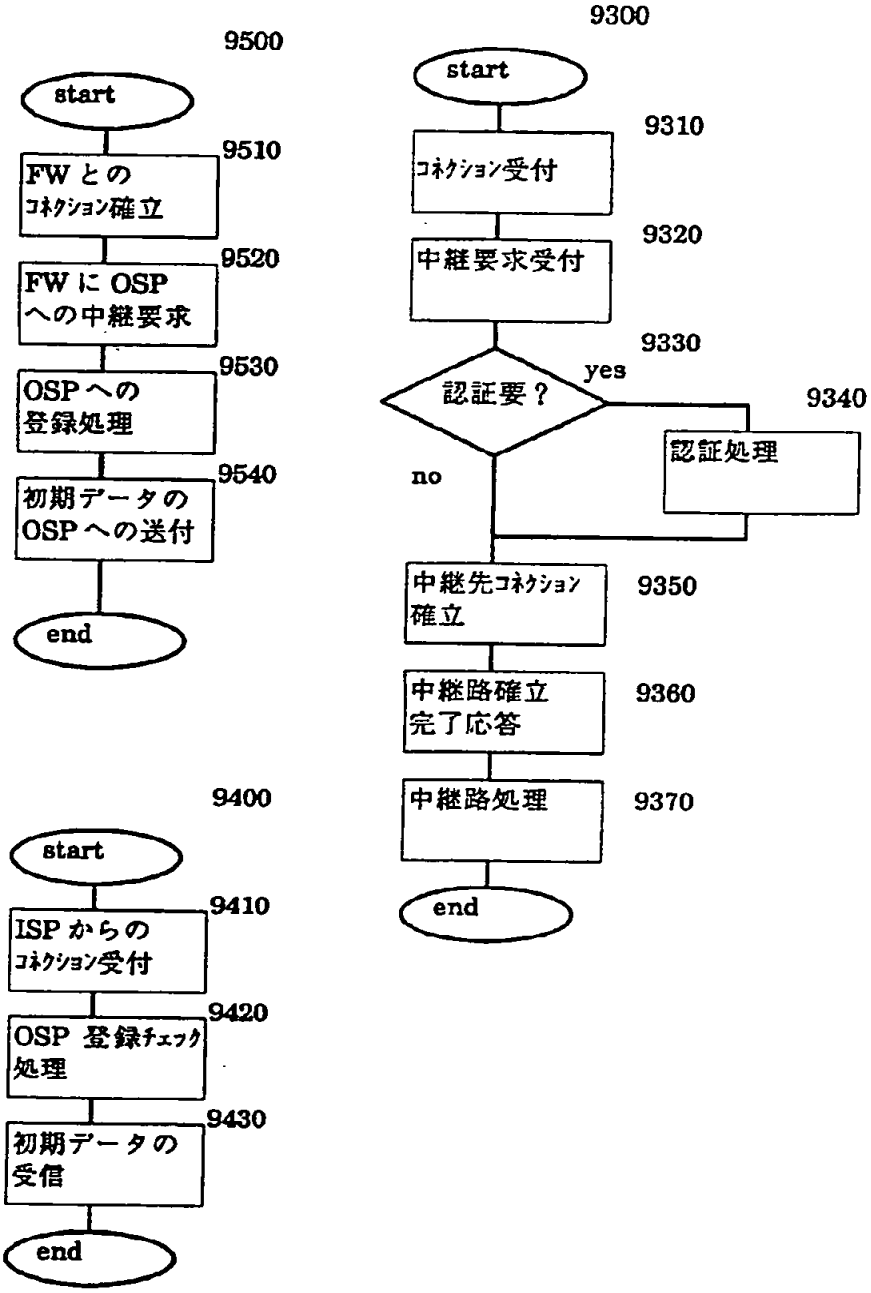
【図２３】

図 23



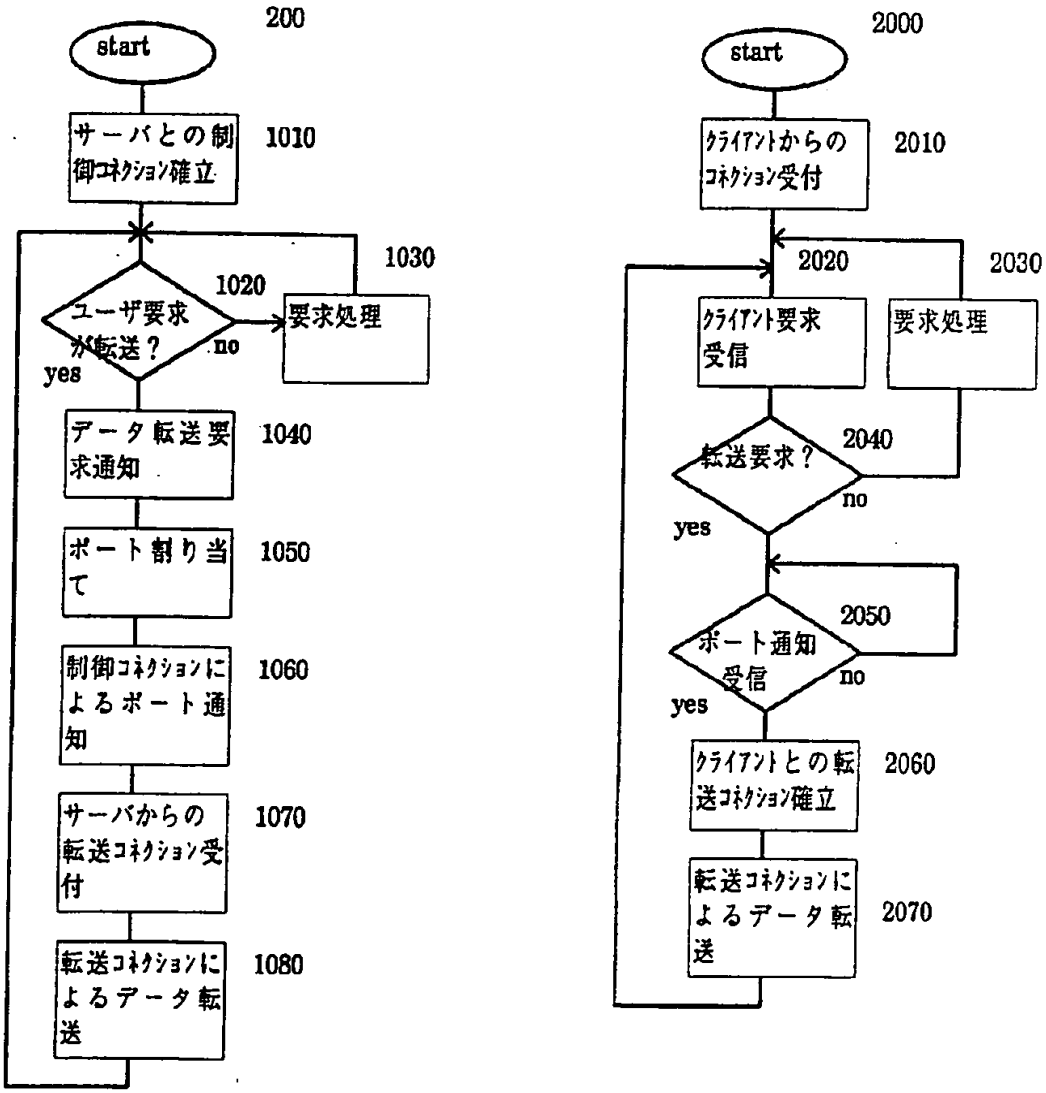
【図９】

図 9


9500
start
9510
FW との
コネクション確立
9520
FW に OSP
への中継要求
9530
OSP への
登録処理
9540
初期データの
OSP への送付
end
9300
start
9310
コネクション受付
9320
中継要求受付
9330
認証要？
yes
9340
認証処理
no
中継先コネクション
確立
9350
中継路確立
完了応答
9360
中継路処理
9370
end
9400
start
9410
ISP からの
コネクション受付
9420
OSP 登録チェック
処理
9430
初期データの
受信
end

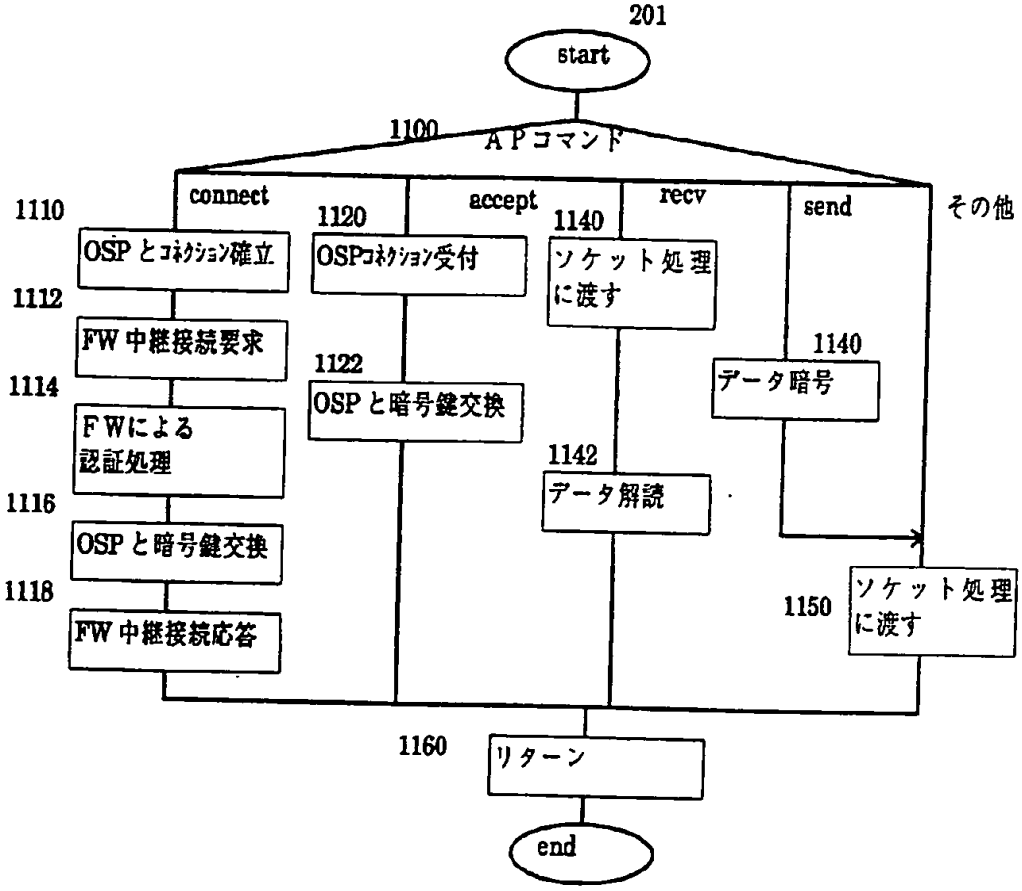
【図１０】

図 10

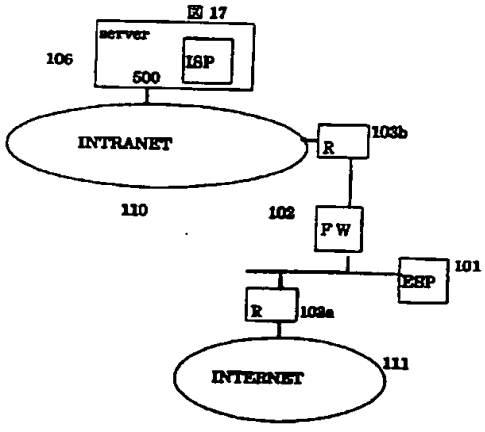

200
start
サーバとの制御コネクション確立
1010
1020
ユーザ要求が転送？
no
yes
1030
要求処理
データ転送要求通知
1040
ポート割り当て
1050
制御コネクションによるポート通知
1060
サーバからの転送コネクション受付
1070
転送コネクションによるデータ転送
1080
2000
start
クライアントからのコネクション受付
2010
2020
2030
クライアント要求受信
要求処理
転送要求？
2040
no
yes
2050
ポート通知受信
no
yes
クライアントとの転送コネクション確立
2060
転送コネクションによるデータ転送
2070

【図１１】

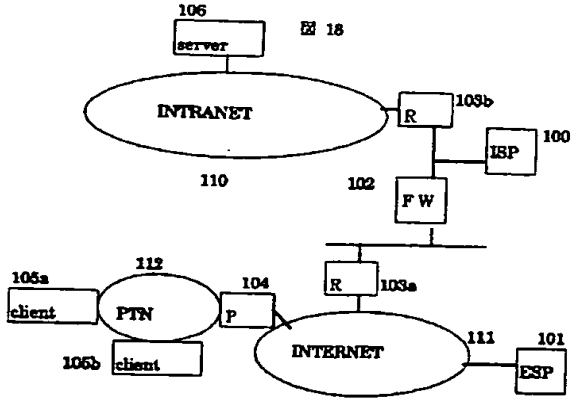
図 11



【図１７】

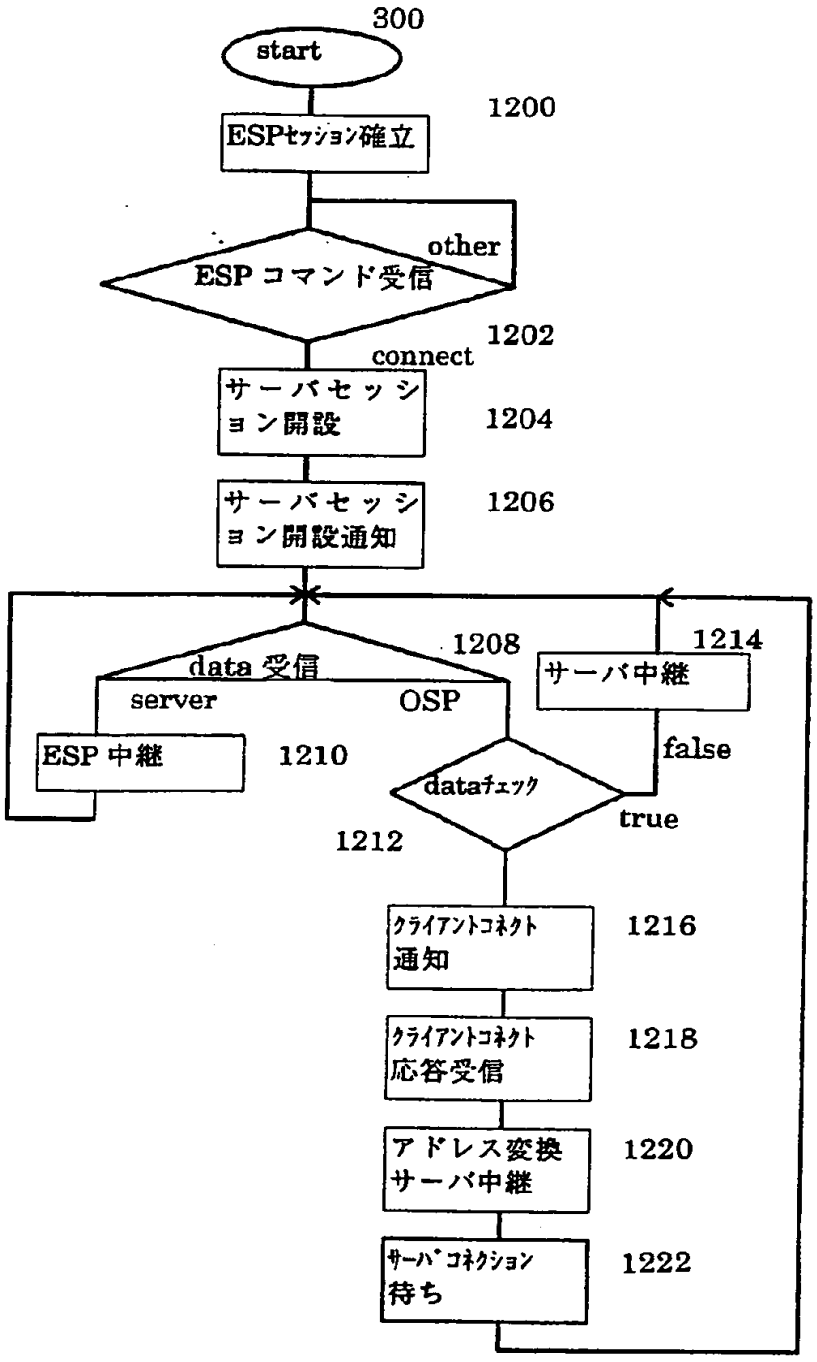


【図１８】



【図１２】

図 12



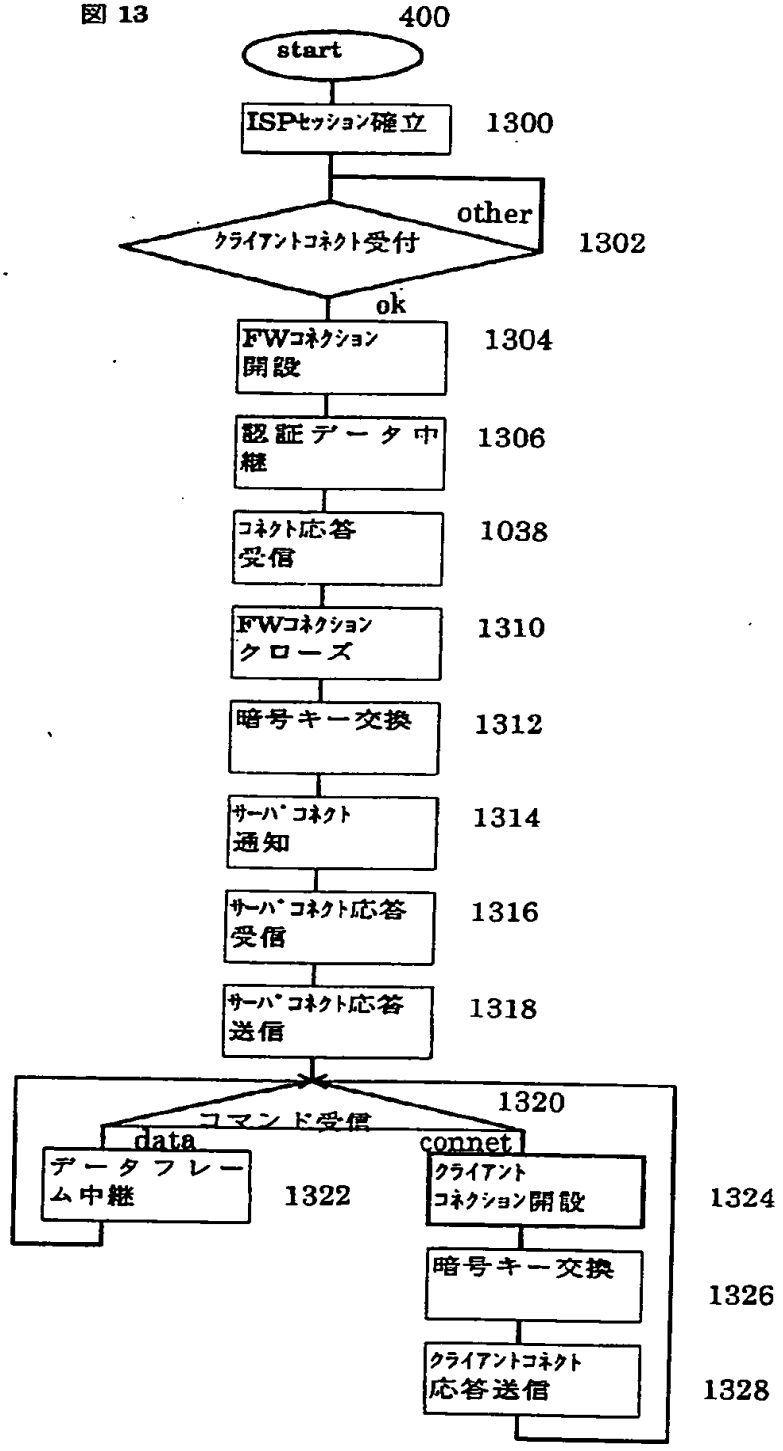
【図２２】

図 22

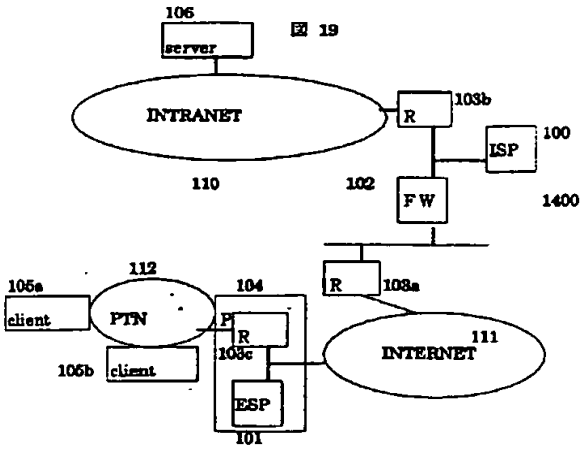
```
#  AP  ACCESS  CONTOROL  MACRO
initial service-address  =  xxx.xxx.xxx.xxx.yyy.yyy
ISP part
{
 if  (Top_Data == "PORT")
 {
   Change_address;
   Accept;
   Send p1;
   if ( Recv p2)    { Forward_I; }
 }
}

ESP part
{
 if(Recv p1)
 {
  Connect;
  Key_Change;
  Send p2;
  Forward_E;
 }
}
```

【図１３】

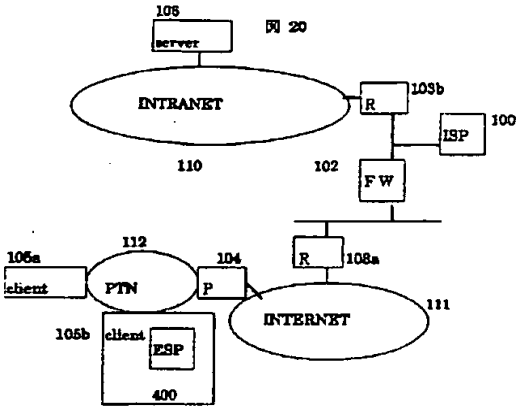
図 13


400
start
ISPセッション確立
1300
other
クライアントコネクト受付
1302
ok
FWコネクション開設
1304
認証データ中継
1306
コネクト応答受信
1038
FWコネクションクローズ
1310
暗号キー交換
1312
サーバコネクト通知
1314
サーバコネクト応答受信
1316
サーバコネクト応答送信
1318
1320
コマンド受信
data
connet
データフレーム中継
1322
クライアントコネクション開設
1324
暗号キー交換
1326
クライアントコネクト応答送信
1328

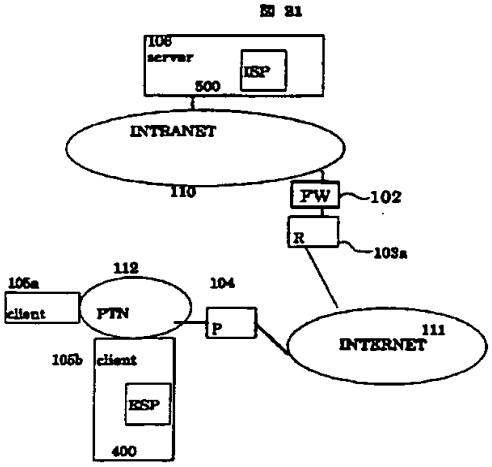
【図１９】



【図２０】



【図２１】



フロントページの続き

(51) Int. Cl. ⁶	識別記号	F I
H04L 12/24		
12/26		